AO-106 (Rev: 06/09)-Application for Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of **In the Matter of the Search of Information Associated with the Google Accounts bjmclurd11@gmail.com and larrysilber@gmail.com that are Stored at a Premises Controlled by Google LLC**	Case No. 24-MJ-313-MTS **FILED UNDER SEAL**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	**Wire Fraud**
18 U.S.C. § 1344	**Bank Fraud**

The application is based on these facts:

See Affidavit of TFO Andrew Titsworth, HSI attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrew Titsworth
Applicant's signature

TFO Andrew Titsworth, HSI
Printed name and title

Subscribed and sworn to by phone.

Date: 4-30-2024

Judge's signature

City and state: Tulsa, Oklahoma

U.S. Magistrate Judge Mark T. Steele
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Information Associated with the Google Accounts bjmclurd11@gmail.com and larrysilber@gmail.com that are Stored at a Premises Controlled by Google LLC	**Case No. _____** **FILED UNDER SEAL**

Affidavit in Support of an Application for a Search Warrant

I, Andrew Titsworth, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at a premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Task Force Officer (TFO) with Homeland Security Investigations (HSI), within the Department of Homeland Security (DHS), assigned to the Tulsa, Oklahoma Resident Agent in Charge Office. I have been so assigned since May 2019. As part of my duties as an HSI TFO, I investigate criminal violations relating to smuggling goods into the United States, wire fraud, fraud schemes, and various financial crimes. Prior to being assigned to the HSI Task Force, I have been a Deputy Sheriff at the Tulsa County Sheriff's Office (TCSO) since December 2010. I completed the HSI TFO training program in Lorton, Virginia, where I received training relative to intellectual property rights, conspiracy investigations, child pornography investigations, general smuggling investigations, smuggling of arms and strategic technology, and various surveillance and investigative techniques.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted

for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of **18 United States Code § 1343 (Wire Fraud) and 18 United States Code 1344 (Bank Fraud)** have been committed by Rodney CLIFTON and others. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes, as further described in Attachment B.

Jurisdiction

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

6. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Google from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate,

where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

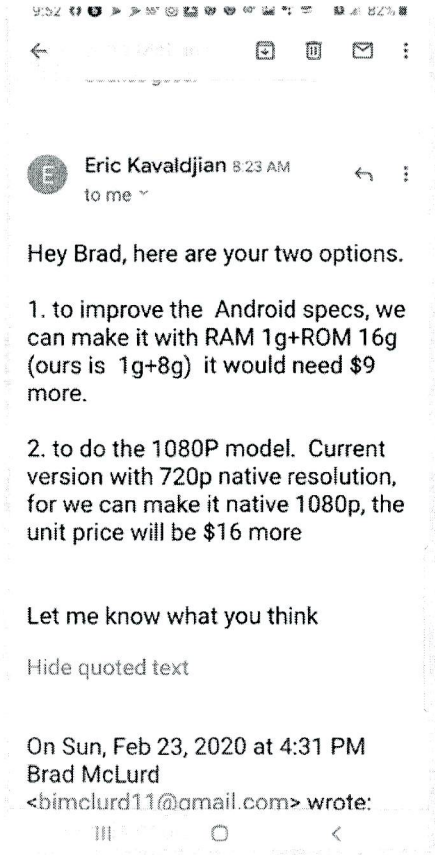
Probable Cause

7. In February 2024, Homeland Security Investigations (HSI) Tulsa was requested to assist the Tulsa County Sheriff's Office (TCSO) with a criminal investigation of a group of conspirators called Deep East Texas Sound and Vision (DETSAV). The Oklahoma Attorney General in coordination with TCSO are currently pursuing charges against the members of DETSAV who are violating the Oklahoma Racketeering Influenced and Corrupt Organization Act (RICO Act), as well as other state crimes. The scam involved multiple co-conspirators selling inferior television projectors that were packaged in boxes displaying descriptions of a much higher quality than the truth. The conspirators would let the victims read the packaging so that they would infer the product was as advertised. The victim could also scan a QR code on the side of the projector boxes to access websites that purported to show the MSRP and features of the projector. The conspirators would then sell the inferior projector at prices the conspirators represented as cheaper than if they bought it elsewhere. In the Northern District of Oklahoma, at least ten individuals have fallen victim to the scam.

8. Evidence relating to transactions of this scam reveals likely violations of 18 United States Code § 1343 (Wire Fraud) and 18 United States Code 1344 (Bank Fraud) wherein the conspirators have made material misrepresentations orally

and/or through the use of websites reflecting false information to obtain money or property by wire transaction or bank check.

9. One conspirator, Rodney CLIFTON, was arrested in late 2022 in the state of Texas on unrelated Organized Crime charges. The League City Police Department, in Texas, obtained a Search Warrant for a cellular phone in CLIFTON's possession at the time of his arrest. Because they found evidence of crimes committed in Oklahoma, the League City Police Department gave a copy of the forensic download of that cellular device to TCSO Deputy Hirsch. Deputy Hirsch's review of that digital download revealed evidence of several crimes, including fraud and violations of the Oklahoma RICO Act, being committed in Tulsa County. Specifically, Deputy Hirsch found screenshots of emails that were sent to CLIFTON's phone by fellow conspirator, Bradley MCLURD. These screenshots showed emails between various members of the conspiracy discussing the low-end specifications of the projectors. They also showed the conspirators discussing the representations made on the packaging of the projectors. One such screenshot (below) shows an email account, **bjmclured11@gmail.com** discussing with another email account the low-end specifications of the devices being falsely advertised as high-end, and the cost per unit to make upgrades to the devices. The email exchange is in furtherance of the scheme by attempting to improve the quality of projectors sold, but still not selling the advertised quality of the projector being displayed on the packaging.



Eric Kavaldjian 8:23 AM
to me

Hey Brad, here are your two options.

1. to improve the Android specs, we can make it with RAM 1g+ROM 16g (ours is 1g+8g) it would need $9 more.

2. to do the 1080P model. Current version with 720p native resolution, for we can make it native 1080p, the unit price will be $16 more

Let me know what you think

Hide quoted text

On Sun, Feb 23, 2020 at 4:31 PM Brad McLurd <bimclurd11@gmail.com> wrote:

10. Another screenshot of an email exchange found on CLIFTON's phone shows an email from **larrysilber@gmail.com**, discussing with jimmy@htp.com.cn specific changes to the advertising on the boxes of the projectors. These specific boxes, and the markings, are comparable to fraudulent packaging observed by investigators. As discussed below, CLIFTON was interviewed by law enforcement. In that interview, CLIFTON was asked about this screenshot referencing Silber's gmail.com account. CLIFTON stated **larrysilber@gmail.com** was Larry Silber's gmail account. CLIFTON further stated that Larry Silber is the designer, manufacturer, importer,

distributor, and Office manager for the projector scam. CLIFTON confirmed that members of the conspiracy, including McLurd and Silber, communicate via email regarding the advertisements and packaging of the fraudulent projectors.

11. Through the 2022 League City Police Department search warrant for the cellular phone in CLIFTON's possession, a victim was identified located in the Tulsa area. Deputy Hirsch located the following text message in CLIFTON's phone dated February 3, 2022, which identified Robert Ward as a victim.

> "Hey Rodney, I purchased the McClaron 8K projector and screen from you in Tulsa about a week ago. I have a friend of mine that is going to purchase it from me as like I said I didn't need it, you said your company will warrantee for 5 years if I remember correctly. Is that correct sir? Rob Ward"

12. On January 11, 2023, TCSO Deputy Hirsch met with Robert Ward. Ward stated he was in the parking lot of the Hideaway Pizza at 7549 S. Olympia Ave, Tulsa, OK 74132, in his black 2020 Ford F250 pickup, when he was approached by two White Males in a newer model Chevrolet Suburban. Ward stated the driver was younger, in his 40's and named "Rod", and the passenger was older, possibly in his 50's, but did not exit the vehicle or speak much. Ward stated Clifton told him they were in town from Texas on a job installing projectors and screens at a business in Broken Arrow. Ward stated Clifton was obviously the boss and did all the talking. Ward stated Clifton told him the client for the job didn't need or want some of the projectors, so he was now trying to sell them at a discounted price. Ward stated Clifton was "clean cut" and looked the part. Ward stated Clifton showed him a business card to gain his confidence about his identity. Ward stated Clifton showed

him four or five projectors and screens in the back of their vehicle and told him they were worth $9,000 each. Ward stated Clifton showed him a website showing the price of the projectors at $9,000. Ward stated Clifton told him if he didn't like it, he could resell it for a large profit. Ward stated Clifton originally asked for $3,000, but then settled on $2,500 for one projector and one screen. Ward stated he wrote Clifton a check in the Hideaway parking lot and Clifton wrote him a receipt for the projectors. Ward stated Clifton wrote his name and phone number on the back of the receipt.

13. Ward stated Clifton drove to the bank who issued the check, Security Bank at 10727 E. 51 Street, Tulsa, OK 74146, and immediately cashed the check. Ward surrendered the projector, screen, and receipt to Deputy Hirsch at the time Ward gave his statement alleging he was a victim of a scam, and those items were booked into the Tulsa County Property Room as evidence.

14. Beginning in approximately the summer of 2023 to early 2024, the O'Fallon Police Department (OPD) located in O'Fallon Missouri began receiving reports of victims of the projector scam. Specifically, on February 28, 2024, the OPD took a report from victim Brennan Lograsso who stated that on February 28, 2024, at approximately 0830 hours he was leaving the parking lot of a Home Depot located at 1525 Highway K, O'Fallon, MO, 63366. The victim stated as he was leaving a newer model, white Ford Expedition with Texas plates (TFN1340) approached him. The victim stated a male named "Charlie" exited the vehicle and offered to sell him a

projector and projector screen. The victim advised "Charlie" told him he was in town to deliver projectors for Buffalo Wild Wings but had several extras that he wanted to sell. He identified the projectors as being the same projectors used at Buffalo Wild Wings and having the following specifications: Ennea Projector, Model: E8K-8900, 8K Ultra HD 7680x4320, Cost: $11,200.00, 8 Simultaneous Display screens, Cystal clear, Used for Gaming systems/golf simulators.

15. The victim stated a QR code on the projector's box took him to the following link, Ennaprojectors.com/e8k-8900. The link provided the following description of the above stated projector: Price: $11,999.99 SPECIAL FEATURES, Optimized Light Engine, Advanced Picture with Digital Video, Noise Reduction, 25dB Ultra Quiet Fan, 5" LCD TFT Display, 0.8 Ratio Short Throw, Native contrast ratio: 40000:1, 250 Watt Ultra Bright Lamp, Color Temperature 9000K, Lamps Power: 250W/100,000 Hours, Nominal Impedance: 4-8 Ohms, DISPLAY TECH, Projector system: 8k laser tech Lamp, HDMI & Video Cable, Digital HDMI Projector, Brightness: 8000 Lumens.

16. The victim stated "Charlie" informed him that the projectors were very expensive, but he would be willing to give him a deal. He stated, after negotiations between he and "Charlie," they agreed on the price of $800.00 for the Ennea E8k-8900 and a "Zero Edge Motorized Screen SI-72." The victim stated Charlie attempted to have him pay via a Cashapp with the phone number of 832-998-0923.

Investigative steps confirmed that this phone number was related to an account in the name of Rodney Clifton.

17. The victim stated that he decided to pay in cash, so "Charlie" and an additional unknown subject, currently believed to be Cole Meadows, inside the Ford Expedition followed him to the Bank of America located in O'Fallon, MO where the victim removed and provided $800.00 to "Charlie." "Charlie" in turn provided the victim with a receipt branded under the company name of "Sound Vision" detailing the sale of one Ennea Projector Television and one HD-72 Projection Screen 72" labeled Order #: NE51006150.

18. The victim stated that after he left the area, he conducted an internet search of the above stated projector and learned that the projector was likely fake. He stated he attempted to recontact "Charlie," but was unsuccessful. The victim stated he was scared that he was lied to resulting in him paying far too much money for a fraudulent product. The victim provided copies of the receipt of transaction, turned over the product, and a completed a written statement to OPD.

19. OPD Officer Frkovic conducted an internal computer check in reference to similar cases which resulted in identifying two similar OPD cases.

20. Both OPD cases involved conspirator Rodney CLIFTON approaching subjects in the parking lot of businesses and selling projectors. In one case, the reporting party had the projector professionally reviewed, resulting in a

determination that the product was extremely low quality and retailed for around $150-200.

21. In response to Lograsso's report, on February 28, 2024, OPD Officer Frkovic conducted a review of Flock cameras which revealed the suspect vehicle was still in the area of St. Louis County (Sunset Hills). OPD Officer Frkovic contacted O'Fallon communication officers and had them dispatch officers with the Sunset Hills Police Department in an attempted to locate the vehicle and potential suspects. The Sunset Hills Police Department was able to locate the vehicle and contacted OPD.

22. On February 28, 2024, OPD Detectives Nelson and Judge responded to the vehicle at 10760 Sunset Hills Plaza, Sunset Hills, MO. Detective Judge made contact with CLIFTON at the driver's side of the vehicle and placed CLIFTON under arrest for the state of Missouri charge of Stealing $750 or more. The passenger/co-conspirator was identified as Cole MEADOWS. The vehicle had numerous projectors and projection screens resting in the back seat and rear cargo area of the SUV. Detective Judge further observed the packaging for the A/V equipment to match the fraudulent projector and projection screen that was purchased by Lograsso.

23. The white Ford Expedition with Texas plates (TFN1340) was registered to Enterprise Holdings, LLC 14002 East 21st St Suite 1500 Tulsa, OK 74134. The vehicle was towed to Budget Towing pending a search warrant application. A black

iPhone in a black pelican case was seized on CLIFTON's person incident to his arrest.

24. On February 29, 2024, OPD Detective Lohmeyer submitted a search warrant application to the St. Charles County Prosecuting Attorney's Office, Judge Sandcork authorized a search of the silver Ford Expedition TX/TFN1340. OPD recovered twelve (12) Ennea E8K-8900 8K Ultra HD Projectors, twelve (12) Zero Edge SI-72 motorized screen projector, (1) Samsung Android phone with black speck case S/N: R58W417EKKX, (1) Apple iPhone mini with black otter case, miscellaneous receipts, itemized Sound Vision receipts, and invoices for Sound Vision with payment methods documented.

25. On February 29, 2024, agents and detectives from TCSO, the Oklahoma Attorney General's Office, OPD, and HSI, conducted an interview with CLIFTON at OPD, O'Fallon, Missouri. In the recorded interview with CLIFTON, post Miranda and signing a Rights Waiver, CLIFTON admitted he was aware of the fraudulent nature of the projectors while performing the scam.

26. During the interview CLIFTON described selling the projectors as wholesaling and stated that he has been doing it for around twelve years. CLIFTON defined wholesaling as independently purchasing the low-quality projectors, or other electronic devices, from a warehouse to sell, or working for a business, called an "Office," and selling the devices that the Office provided.

27. CLIFTON also stated an Office was a company or business owned by an individual, whereby that individual would buy the devices from a warehouse, and several salespersons would work for the Office selling the devices it purchased. CLIFTON stated there were high-level people that were in charge of designing, manufacturing, importing, and distributing the devices nation-wide. CLIFTON named several of those people: McLurd, Silber, Nigel, LA Logistics, Canadian Eric, and Jack Amaroso, but stated there were many more that he could not name. CLIFTON stated these high-level people would all make different versions of the projectors, giving Offices and independent salespersons hundreds to choose from. CLIFTON stated these high-level people would inform the warehouses of the devices that they made and would pay the warehouses to hold their devices so independent salespersons and Offices could acquire them from the warehouse. CLIFTON stated the warehouses would even deliver the devices to the Offices because the Offices bought in such high quantities. CLIFTON stated that on top of the designing, manufacturing, importing, and distributing of devices, Larry also ran Offices in multiple cities and states in the United States.

28. CLIFTON said that he initially started working in one of the Offices but eventually graduated training and became a trainer for the Office. After working in the Office, CLIFTON opened his own business selling the projection devices. CLIFTON said he would sell the devices in any major city. CLIFTON resides in the Houston area, and the farthest he traveled west for sales was Salt Lake City, Utah;

the farthest east was Charlotte, North Carolina; and the farthest north for sales was Fargo, North Dakota.

29. Concerning the fraudulent representations for the projection devices, CLIFTON stated all the devices have capabilities and specifications printed on the packaging and written on websites associated with the "brand" of the device. CLIFTON stated you can find these websites by searching for them online, or by scanning a QR code on the box that takes you directly to the websites. CLIFTON gave an example of this with the "brand" of projector he was selling in February 2024 in Missouri. CLIFTON stated the "brand" was Ennea and you could go to EnneaProjectors.com to read a "write-up" on the projector and the screen that came with it. CLIFTON stated that along with the capabilities and specifications, the packaging and websites also had a MSRP for each device, which is hyper-inflated. CLIFTON stated that the hyper-inflated MSRP for the projectors ranges from $4,000 to $11,000. CLIFTON stated several times that he would show the victims the hyper-inflated MSRP for the devices, but he would tell them "MSRP don't mean nothing, that's just the suggested retail price," and that he could sell the projectors for whatever he wants to sell them for. When asked how CLIFTON convinces people they are buying a "high quality product," CLIFTON stated he relies on the website with the specifications and the "write-up," as well as plugging the device in to show them it works. CLIFTON describes what he does as "hustling," or "hustling on the street." CLIFTON stated he doesn't like that he has to hustle, and he claimed he and

Joshua Frank made a plan to make as much money as possible selling projectors before moving on to a different line of work over the last three years.

30. TCSO Deputy Hirsch confronted CLIFTON about four specific dates whereon CLIFTON is believed to have sold fraudulent projectors in or Tulsa, Oklahoma: December 8th, 2021, December 22nd, 2021, January 4th, 2022, and January 25th, 2022. Deputy Hirsch's conversation with CLIFTON about these instances elicited the following materially relevant responses:

a. Deputy Hirsch asked CLIFTON if a victim wrote CLIFTON a check on January 25th, 2022, for the sale of a projector. CLIFTON admitted many of his victims write him checks. Deputy Hirsch asked if it would surprise him that he was written a check on that date and CLIFTON stated "No, absolutely not." CLIFTON explained that he normally would cash the check immediately in person if the victim's bank branch is close by but would also mobile deposit the check if no bank branches were available.

b. Deputy Hirsch showed CLIFTON a copy of a check that was obtained by a search warrant concerning victim Robert Ward's bank account at Security Bank, written to "Rodney Clifton," with a memo line stating: "for Sound & Vision 8k laser screen & TV." CLIFTON admitted that the endorsement on the check was in fact CLIFTON's signature and that a series of letters and numbers written at the top of the check reflect

his Texas driver's license number, birthday, and likely the expiration date of his driver's license.

c. Deputy Hirsch informed CLIFTON that the evidence collected in the investigation appears to reflect a pattern of CLIFTON targeting males in nicer parts of town with nice pickup trucks. CLIFTON responded: "I go for country guys, cause they're more safer. I don't go to the ghetto and sell. I'll ask – co – country guys are more safer, so I'll ask them."

d. CLIFTON further acknowledged that he routinely split the proceeds of the sales with others involved in the scheme and explained that it was too difficult to estimate how much money he makes in any given period of time but stated that $3,000 a week was a good week and that his best week was around $4,500 in sales.

31. As noted above, League City Police Department previously obtained a search warrant for a cellular phone in CLIFTON's possession in 2022. The forensic downloads revealed evidence of the scheme to defraud victims through Oklahoma by the sales of low-quality projectors, marketed as being high-end. By CLIFTON's own admissions and arrest in Missouri in February 2024, it is apparent that CLIFTON had not stopped committing the fraud. Investigators believe it is probable that evidence of the conspiracy to commit wire fraud and bank fraud will exist on co-conspirator MCLURD's and SILBER's email accounts of bjmclurd11@gmail.com and larrysilber@gmail.com as discussed herein.

Background Concerning Google[1]

32. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

33. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

34. Signing up for a Google Account automatically generates an email address at the domain "gmail.com." That email address will be the log-in username for access to the Google Account.

35. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

36. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

37. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

38. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

39. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

40. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

41. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

42. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

43. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators or other social

media platforms. Social media platforms such as YouTube are often linked to other accounts or phone numbers utilized in furtherance of criminal activity. This investigation has revealed a screenshot of an email conversation showing a picture taken and possibly altered from an application used to create box templates to display false advertising on the fraudulent devices. Information stored by Google relating to applications accessed, modified, or downloaded by these accounts can reveal the methods used in altering, modifying, creating and manufacturing the fraudulent devices and/or the boxes housing the fraudulent devices, as well as identifying co-conspirators involved in these activities. The investigation also shows CLIFTON, MCLURD, and SILBER used text messaging apps and/or instant messaging apps to send text, videos, and pictures to each other and to other co-conspirators as forms of communication about the conspiracy. Collection of data relating to the sending or receiving of text, videos, pictures and other media through applications associated with Google accounts can contain data or evidence of currently crimes under investigation. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

44. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email

addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

45. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar, so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

46. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the

messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

47. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups

on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

48. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

49. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

50. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

51. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

52. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called "My Activity."

53. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a

Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts into automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

54. Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

55. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

56. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. Specifically, Google's servers are likely to contain stored electronic communications and information relating to the bjmclurd11@gmail.com account and their email communications with various co-conspirators or other persons involved in the design, manufacture, procurement, shipping, receiving and distribution of fraudulent devices utilized in the conspiracy. The stored electronic communications and information relating to the bjmclurd11@gmail.com account can reveal content and context for communication between conspirators, as well as the coordination, action and activities of those conspirators. The stored electronic communications and information relating to the bjmclurd11@gmail.com account can also reveal monetary transactions, both collection and distribution, as relating to the conspiracy, and the methods thereof. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users and location-based data.

Information to be Searched and Things to be Seized

57. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it,

reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

58. Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

59. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crimes under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, Affiant knows that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text.

Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

60. Based on the information above, I submit that there is probable cause for a search warrant authorizing search of the Google account data, as described in Attachment B.

61. I request to be allowed to share this affidavit and the information obtained form this search with any government agency, to include state and local agencies investigating or adding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclose obligations in any prosecutions from this matter.

Respectfully submitted,

Andrew Titsworth

Andrew Titsworth
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to by phone on April 30, 2024.

MARK T. STEELE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with bjmclurd11@gmail.com and larrysilber@gmail.com ("the Accounts") that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f). Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from February 1, 2020 to April 29, 2024, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Accounts, including:

1. Names (including subscriber names, user names, and screen names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3. Telephone numbers, including SMS recovery and alternate sign-in numbers;

4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS

recovery numbers, Google Voice numbers, and alternate sign-in numbers;

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Accounts, including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs.

d. The contents of all emails associated with the Accounts, including stored or preserved copies of emails sent to and from the Accounts, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails. All forwarding or fetching accounts relating to the accounts;

e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

f. Any records pertaining to the user's calendars, including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

g. The contents of all text, audio, and video messages associated with the Accounts, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

h. The contents of all records associated with the Accounts in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists,

i. The contents of all media associated with the Accounts in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the Accounts, including drafts and deleted records; Accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

j. All maps data associated with the Accounts, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the Accounts; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

k. All Location History and Web & App Activity indicating the location at which the Accounts were active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

l. All payment and transaction data associated with the Accounts, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history;

m. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

n. All Google Voice records associated with the Accounts, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings and all associated logs, including access logs, IP addresses, location data, timestamps, and change history;

o. All records or other information regarding the identification of the Accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

p. The types of service utilized;

q. All records or other information stored by an individual using the Accounts, including address books, contact and buddy lists, calendar data, pictures, and files; and

r. All records pertaining to communications between Google and any person regarding the Accounts, including contacts with support services and records of actions taken.

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 United States Code § 1343 (Wire Fraud) and 18 United States Code 1344 (Bank Fraud), including, for each account or identifier listed on Attachment A:

a. Communications between Rodney CLIFTON, Bradley MCLURD, or Larry Silber with co-conspirators about the purchase, distribution, and sales tactics involved in the sub-quality projector sale scheme.

b. Evidence indicating how and when the Accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the Account owner's state of mind as it relates to the crimes under investigation;

d. The identity of the persons who created or used the Accounts, including records that help reveal the whereabouts of such persons.

e. The identity of the persons who communicated with the Accounts about matters relating to wire fraud and bank fraud including records that help reveal their whereabouts.

Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ .

I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. Such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature